EXPEDITED PROCEDURE UNDER 37 CFR § 1.116
GROUP ART UNIT 2137; EXAMINER Z. Davis
PATENT
***IBM Docket No.* POU920000179US1 09/740,457**

Amendment to Specification

Please update the first paragraph, lines 1-8, on page 3 of the subject application as follows:

The multiplication of binary numbers modulo [module] *N* is an important operation in modern, public-key cryptography. The security of any cryptographic system which is based upon the multiplication and subsequent factoring of large integers is directly related to the size of the numbers employed, that is, the number of bits or digits in the number. For example, each of the two multiplying factors may have up to 1,024 bits. However, for cryptographic purposes, it is necessary to carry out this multiplication modulo a number *N*. Accordingly, it should be understood that the multiplication considered herein multiplies two n bit numbers to produce a result with *n* bits or less rather then the usual 2*n* bits in conventional multiplication.